(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－140235
(P2002－140235A)
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｋ　５Ｂ０１７

審査請求　有　請求項の数６　ＯＬ　（全５頁）

(21)出願番号　特願2000－335336(P2000－335336)

(22)出願日　平成12年11月２日(2000.11.2)

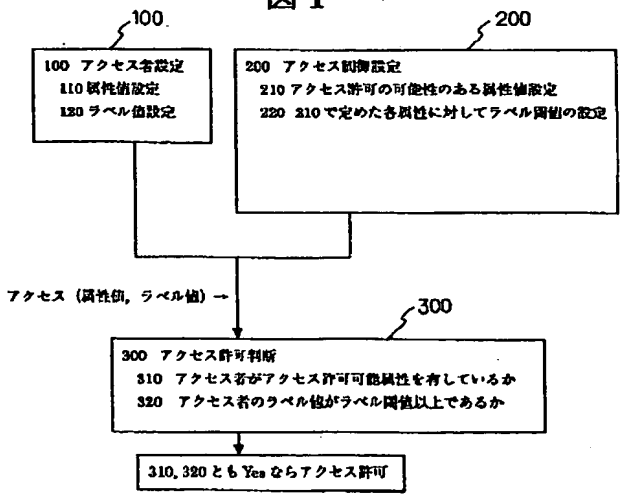
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　可児島　建
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083552
弁理士　秋田　収喜

Ｆターム(参考)　５Ｂ０１７ ＡＡ０７ ＢＡ０６ ＢＢ０６ ＣＡ１６

(54)【発明の名称】　アクセス制御方法及び装置並びにそのプログラムの記録媒体

(57)【要約】
【課題】　アクセス者の条件及び被アクセス区分の条件の双方に基づくアクセス制御を可能にする。
【解決手段】　情報システムへのアクセスを制御する方法におけるアクセス制御設定方法であって、アクセス制御対象情報及びそれへの操作種別の組合せを被アクセス区分とするとき、各被アクセス区分に対応させるアクセス許可可能属性を設定し、その後、前記被アクセス区分と前記アクセス許可可能属性の組合せに対して、ラベル閾値を設定するものである。

図１



【特許請求の範囲】
【請求項１】情報システムへのアクセスを制御する方法に用いるアクセス制御設定方法であって、アクセス制御対象情報及びそれへの操作種別の組合せを被アクセス区分とするとき、各被アクセス区分に対応させるアクセス許可可能属性を設定し、その後、前記被アクセス区分と前記アクセス許可可能属性の組合せに対して、ラベル閾値を設定することを特徴とするアクセス制御設定方法。
【請求項２】請求項１に記載のアクセス制御設定方法の処理手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項３】請求項１に記載のアクセス制御設定方法により、アクセス者が被アクセス区分にアクセスを試みた場合のアクセス制御する方法に用いるアクセス許可判断方法であって、前記アクセス者の属性が、その被アクセス区分の許可可能属性かどうかを判断し、その後、前記アクセス者に与えられているラベル値が、その被アクセス区分とアクセス許可属性に対応づけられたラベル閾値以上であるかどうか判断し、双方の判断が是とされたとき、そのアクセスを許可することを特徴とするアクセス許可判断方法。
【請求項４】請求項３に記載のアクセス許可判断方法の処理手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項５】情報システムへのアクセスを制御するアクセスを制御装置に用いるアクセス制御設定装置であって、アクセス制御対象情報及びそれへの操作種別の組合せを被アクセス区分とするとき、各被アクセス区分に対応させるアクセス許可可能属性を設定するアクセス許可可能属性設定手段と、前記被アクセス区分と前記アクセス許可可能属性の組合せに対して、ラベル閾値を設定するラベル閾値設定手段を備えたことを特徴とするアクセス制御設定装置。
【請求項６】請求項５に記載のアクセス制御設定装置により、アクセス者が被アクセス区分にアクセスを試みた場合のアクセス制御装置に用いるアクセス許可判断装置において、前記アクセス者の属性が、その被アクセス区分の許可可能属性かどうかを判断する許可可能属性判断手段と、前記アクセス者に与えられているラベル値が、その被アクセス区分とアクセス許可属性に対応づけられたラベル閾値以上であるかどうか判断するラベル閾値判断手段と、双方の判断が是とされたとき、そのアクセスを許可するアクセス許可手段とを備えたことを特徴とするアクセス許可判断装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報へのアクセス制御方法及び装置並びにそのプログラムの記録媒体に関し、特に、前記アクセス制御方法及び装置に用いるアクセス制御設定とアクセス許可判断に適用して有効な技術に関するものである。
【０００２】
【従来の技術】従来のアクセス制御方法には、（１）アクセスコントロールリスト（ＡＣＬ）によるものと、（２）ラベルによるものとの２種類がある。前記アクセス制御方法（１）におけるアクセス制御設定方法は、被アクセス区分に、アクセス許可属性値の有限長リストを対応づけし、アクセス者にも属性値を割り当てておく方法であり、また、アクセス許可判断方法は、「アクセスが許可される必要十分条件は、アクセス者に割り当てられている属性値が、被アクセス区分に対応づけられているアクセス許可属性値の内の一つに一致すること」とするものである。また、前記アクセス制御方法（２）におけるアクセス制御設定は、何らかの順序集合（Ｌ，≧）をまず定め、それを利用する。各々の被アクセス区分に、閾値とするＬの一要素（「ラベル」という）ｌを対応づけ、アクセス者にもＬの一要素ｌ’をラベルとして割り当てる設定を行なうものである。この場合のアクセス許可判断方法は、「アクセスが許可される必要十分条件は（前記の記号を用いて）ｌ’≧ｌ」である。
【０００３】
【発明が解決しようとする課題】前記アクセス制御をアクセス者属性とある順序集合のラベルの組合せ条件で行ないたい場合のアクセス制御設定の方法、及びアクセス許可判断の方法は、例えば、オペレータの情報システムへのアクセス制御を行なう場合、部所という属性とオペレータ経験年数というラベルの双方をアクセス制御の判断材料に使用するには、前記アクセス制御方法（１），（２）の各単独方法に帰着させるには、属性をラベルに変換するか、またはその逆の１対１変換が必要となり、無理がある。
【０００４】前記アクセス制御方法（１）のＡＣＬによる方法では、例としてある部課ｃの５年以上の経験年数をもつオペレータのアクセス許可属性を設定する個所において、＜ｃ，５＞，＜ｃ，６＞，…，＜ｃ，５０＞（５０年を仮の限度として）という具合に、許可属性リストが非常に長くなってしまい、非効率な表現が必要となる。また、前記アクセス制御方法（２）のラベルによる方法で同じ例を扱うには、部課と経験年数という性格の異なる属性とラベルの組を要素とする一つの順序集合として表現することが必要となるが、この順序集合は意味付けが不明確でアクセス制御設定が覚束なくなる恐れがある。また、前記例で経験年数の上限がない場合（ラベル集合が無限集合である場合）、前記アクセス制御方法（１）を用いようとしても、ラベルの有限な属性リストへの１対１変換は不可能あり、ＡＣＬの方法に帰着させることができない。
【０００５】本発明の目的は、アクセス者の条件及び被アクセス区分の条件の双方に基づくアクセス制御が可能な技術を提供することにある。本発明の前記ならびにそ

の他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかにする。

【０００６】

【課題を解決するための手段】本願において開示される発明の概要を簡単に説明すれば、下記のとおりである。

（１）情報システムへのアクセスを制御する方法におけるアクセス制御設定方法であって、アクセス制御対象情報及びそれへの操作種別の組合せを被アクセス区分とするとき、各被アクセス区分に対応させるアクセス許可可能属性を設定し、その後、前記被アクセス区分と前記アクセス許可可能属性の組合せに対して、ラベル閾値を設定するものである。

【０００７】（２）前記手段（１）のアクセス制御設定方法の処理手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【０００８】（３）前記手段（１）のアクセス制御設定方法により、アクセス者が被アクセス区分にアクセスを試みた場合のアクセス制御する方法におけるアクセス許可判断方法であって、前記アクセス者の属性が、その被アクセス区分の許可可能属性かどうかを判断し、その後、前記アクセス者に与えられているラベル値が、その被アクセス区分とアクセス許可属性に対応づけられたラベル閾値以上であるかどうか判断し、双方の判断が是とされたとき、そのアクセスを許可するものである。

【０００９】（４）前記手段（３）のアクセス許可判断方法の処理手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００１０】（５）情報システムへのアクセスを制御するアクセスを制御装置におけるアクセス制御設定装置であって、アクセス制御対象情報及びそれへの操作種別の組合せを被アクセス区分とするとき、各被アクセス区分に対応させるアクセス許可可能属性を設定するアクセス許可可能属性設定手段と、前記被アクセス区分と前記アクセス許可可能属性の組合せに対して、ラベル閾値を設定するラベル閾値設定手段を備えたものである。

【００１１】（６）前記手段（５）のアクセス制御設定装置により、アクセス者が被アクセス区分にアクセスを試みた場合のアクセス制御装置におけるアクセス許可判断装置において、前記アクセス者の属性が、その被アクセス区分の許可可能属性かどうかを判断する許可可能属性判断手段と、前記アクセス者に与えられているラベル値が、その被アクセス区分とアクセス許可属性に対応づけられたラベル閾値以上であるかどうか判断するラベル閾値判断手段と、双方の判断が是とされたとき、そのアクセスを許可するアクセス許可手段とを備えたものである。

【００１２】本発明のポイントは、被アクセス区分を１つに特定した場合の、アクセス者ｒのアクセス許可判断までを図１（各項目詳細は図２を参照）のように行う。すなわち、図１に示すように、まず、アクセス者設定（１００）では、アクセス者毎の属性値とラベル値を設定する（１１０，１２０）。

【００１３】また、アクセス制御設定（２００）では、アクセス許可の可能性のある属性値を設定する（２１０）。被アクセス区分に対し、前記ステップ２１０で定めた各属性値ａごとにラベル閾値ｌａを設定する（２２０）。この時ラベル値によらずアクセスを許可しない属性値については、ラベル閾値を設定する必要はない。

【００１４】アクセス許可判断（３００）では、アクセス者ｒの属性値ａ（ｒ）とラベル値ｌ（ｒ）を検出する（３１０，３２０）。ここで、ｒのラベル値が、ｒの属性ａ（ｒ）のラベル閾値$l_{a(r)}$以上であるとき（つまりｌ（ｒ）≧$l_{a(r)}$のとき）、かつそのときに限りアクセスを許可する。なお、アクセス者の属性値は、有限次元ベクトル値も可能である。

【００１５】このようにすることにより、アクセス者の条件及び被アクセス区分の条件の双方に基づくアクセス制御が可能となる。以下に、本発明について、本発明による実施形態（実施例）とともに図面を参照して詳細に説明する。

【００１６】

【発明の実施の形態】図３は、本発明に係る情報システムの概略構成を示すブロック図である。本情報システムは、図３に示すように、複数のアクセス者１からアクセス要求をアクセス制御装置２に入力される。アクセス制御装置２からアクセス者の条件及び被アクセス区分の条件の双方に基づくアクセス制御、例えば、パーソナルコンピュータ（ＰＣ）３、あるいはデータベース（ＤＢ）４、あるいはロボット５等のアクセス制御を行なうものである。前記アクセス制御装置２は、アクセス制御設定装置２１とアクセス許可判断装置２２を有している。

【００１７】図４は、本発明の一実施例の情報システムへのアクセスを制御するアクセス制御装置２におけるアクセス制御設定装置２１の機能構成を示すブロック図である。前記アクセス制御設定装置２１は、図４に示すように、アクセス制御対象情報及びそれへの操作種別の組合せを被アクセス区分とするとき、各被アクセス区分に対応させるアクセス許可可能属性を設定するアクセス許可可能属性設定手段２１１と、前記被アクセス区分と前記アクセス許可可能属性の組合せに対して、ラベル閾値を設定するラベル閾値設定手段２１２を備えている。

【００１８】図５は、本発明の一実施例の情報システムへのアクセスを制御するアクセス制御装置２におけるアクセス許可判断装置２２の機能構成を示すブロック図である。アクセス許可判断装置２２は、図５に示すように、前記アクセス者の属性が、その被アクセス区分の許可可能属性かどうかを判断する許可可能属性判断手段２２１と、前記アクセス者に与えられているラベル値が、

その被アクセス区分とアクセス許可属性に対応づけられたラベル閾値以上であるかどうか判断するラベル閾値判断手段２２２と、双方の判断が是とされたとき、そのアクセスを許可するアクセス許可手段２２３とを備えている。

【００１９】図６は、本発明の一実施の形態におけるアクセス制御設定の一実施例を示す図である。本実施例のアクセス制御設定は、図６に示すように、被アクセス区分は一般に複数ある。また、この例では、図６のラベル順序集合Ｌ＝｛０，１，…，１００｝^{2}における順序は、

【数１】$(e1, e2) \geqq (f1, f2) \Leftrightarrow (e1 > f1) \vee \{(e1 = f1) \wedge (e2 \geqq f2)\}$

と定義できる。

【００２０】アクセス許可判断は、アクセスしようとしている被アクセス区分に、アクセス者のアクセス者属性値が設定されている（被アクセス区分が「Ｒepository１，全操作」の場合はＥngineerとＲesearcherが設定されている）。また、アクセス者のラベルが前記の順序Ｌにおいて、図６に示したラベル閾値以上である（被アクセス区分が「Ｒepository１，全操作」の場合はラベルが（３．０）以上）。という２段階の判断で行われる。

【００２１】以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【００２２】

【発明の効果】以上説明したように、本発明によれば、アクセス者の条件及び被アクセス区分の条件の双方に基づくアクセス制御が可能である。

【図面の簡単な説明】

【図１】本発明によるアクセス制御設定、アクセス許可判断のフローを示す図である。

【図２】図１に示すフロー内部の処理ロジックを示す図である。

【図３】本発明に係る情報システムの概略構成を示すブロック図である。

【図４】本発明の一実施例の情報システムへのアクセスを制御するアクセス制御装置におけるアクセス制御設定装置の機能構成を示すブロック図である。

【図５】本発明の一実施例の情報システムへのアクセスを制御するアクセス制御装置におけるアクセス許可判断装置の機能構成を示すブロック図である。

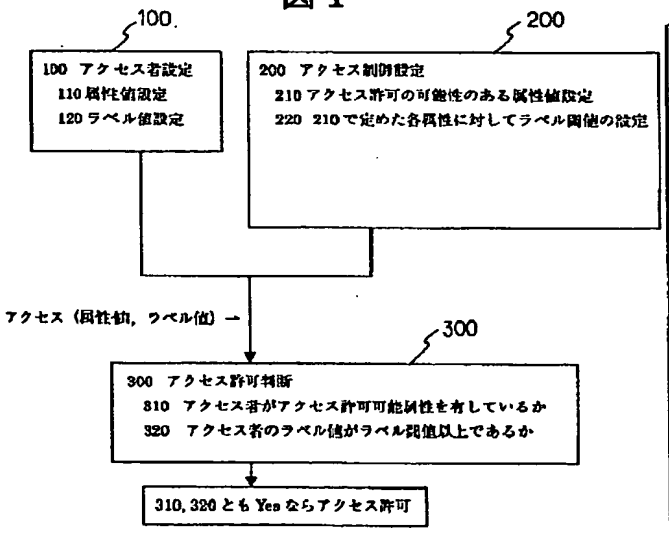
【図６】本発明の一実施の形態におけるアクセス制御設定の一実施例を示す図である。

【符号の説明】

１…アクセス者
２…アクセス制御装置
２１…アクセス制御設定装置
２１１…アクセス許可可能属性設定手段
２１２…ラベル閾値設定手段
２２…アクセス許可判断装置
２２１…許可可能属性判断手段
２２２…ラベル閾値判断手段
２２３…アクセス許可手段
３…パーソナルコンピュータ（ＰＣ）
４…データベース（ＤＢ）
５…ロボット

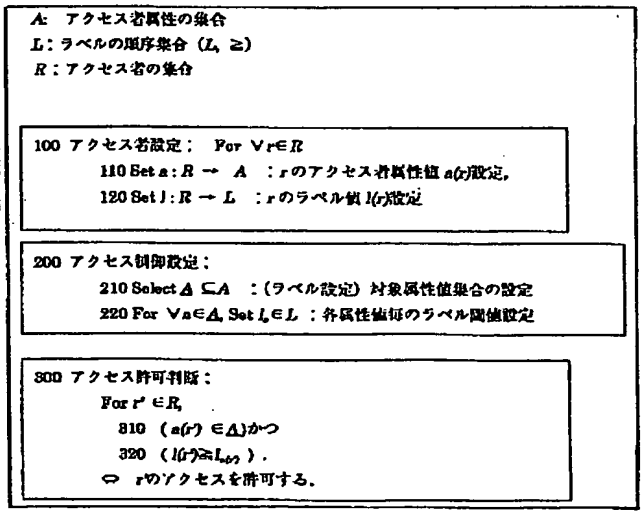
【図１】

図１



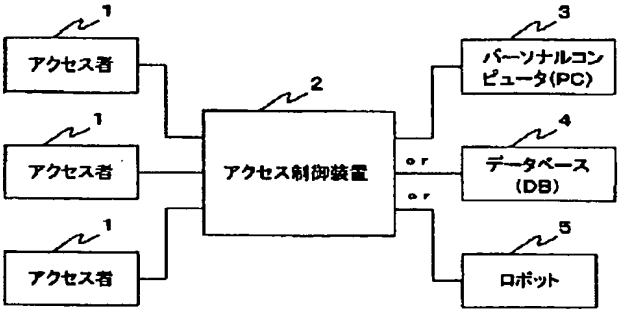
【図２】

図２



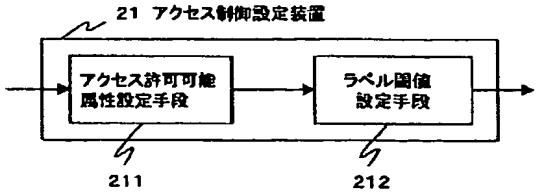
【図３】

図３



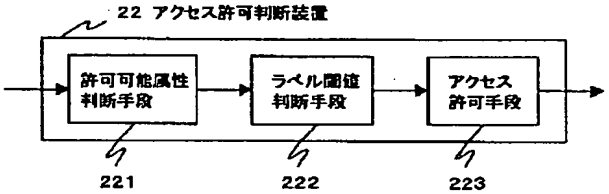
【図４】

図４



【図５】

図５



【図６】

図６

被アクセス区分(r)	アクセス者属性値($a(r)$)	ラベル閾値($l_{a(r)}$)
DataStore1, 新規追加	Manager, Security	(0, 1)
	Manager, Account	(1, 2)
	Staff,*	(5, 0)
	PartTimer,*	(100,0)
DataStore1, 更新	Manager,*	(0, 0)
	Staff,*	(4, 0)
	PartTimer,*	(10, 0)
DataStore1, 参照	Manager,*	(0, 0)
	Staff,*	(1, 0)
	PartTimer,*	(1, 0)
DataStore1, 削除	Manager,*	(1, 0)
	Staff,*	(10, 0)
	PartTimer,*	(100, 0)
Repository1, 全操作	Engineer,*	(3, 0)
	Researcher,*	(3, 0)

凡例("*"表記について)

Staff,* = Staff, Security

or

Staff, Account